TISA Assessment

2006

IT Planning for Quality Assurance	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Compliance
Informational Questions					
A. Estimate the percentage of critical business functions identified in the agency's Business Continuity Plan that have corresponding critical applications enumerated in the agency's annual IT inventory submittal via ISIS.	N/A	N/A	N/A	N/A	
B. Estimate the percentage of projects managed by the agency through a formal IT Quality Assurance program.	N/A	N/A	N/A	N/A	
C. Estimate the percentage of the agency that has incorporated system development lifecycle analysis into their IT planning , budgeting and procurement process.	N/A	N/A	N/A	N/A	
D. Estimate the percentage of the agency that follows a standards-based software development process.	N/A	N/A	N/A	N/A	
E. Estimate the percentage of the agency's adherence to the statewide enterprise architecture policy and standards.	N/A	N/A	N/A	N/A	
F. Estimate the percentage of the agency's adherence to the statewide IT security standards and policy.	N/A	N/A	N/A	N/A	

IT Planning for Data/Information Architecture	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Compliance
S740 DATA MODELING					
A. Estimate the percentage of database/information systems for IT projects that have been through the data modelling process and possess high-level physical data flow diagrams (DFD) meeting the criteria provided in P740. (4.1)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

S741 CLASSIFICATION & CATEGORIZATION OF DATA					
B. Estimate the percentage of data/information systems that are classified according to their degree of sensitivity as either "CONFIDENTIAL" or "PUBLIC" for security purposes. (4.1, 4.2)	N/A	N/A	N/A	N/A	
C. Estimate the percentage of data exchanges being tracked, such as through a Data Exchange file/report identifiying exchange entity names and contacts, application systems, data set name, frequency of exchange, media type, entity type, send/receive status and control status (budget unit or the entity), if the agency shares its data. (4.3)	N/A	N/A	N/A	N/A	
D. Estimate the percentage of databases and/or files identified with risk levels of LOW, MEDIUM, or HIGH for software applications. (4.8)	N/A	N/A	N/A	N/A	
S742 DATABASE ACCESS					
E. Estimate the percentage of database systems that have implemented database security with regard to confidentiality, integrity, and availability of data as established by the S741 Classification and Categorization of Data Standard, and Statewide Policy P800 IT Security, and related statewide security standards. (4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	
F. Estimate the percentage of agency database systems using identification, authentication, authorization, and access controls defined by Network, Security, Platform, and Software Statewide IT standards. (4.12)	N/A	N/A	N/A	N/A	

IT Planning for Network Architecture	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Complian
S710 Network Infrastructure Planning					
A. Estimate the percentage of Structured Cabling Systems standards on new buildings, major cable plant additions or modifications, and/or building renovations based on the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) and Commercial Building Telecommunications Standards 568, 569, 606,607, and applicable electrical codes. (4.1)	N/A	N/A	N/A	N/A	
B. Estimate the percentage of Copper Network Cabling installations for new buildings, major cable plant additions or modifications, building renovations and /or remodeling using Category 5e or Category 6. (4.2)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

C. Estimate the percentage of multi-mode or single-mode Fiber Network Cabling installations for new buildings, major cable plant additions or modifications, building renovations and/or remodeling used by the agency. (4.3)	N/A	N/A	N/A	N/A	
D. Estimate the percentage of the agency's Wireless Network Connectiviity that is secure in accordance with Statewide Standard P800-S830, Network Security; uses encryption technologies; is protected by Virtual Private Network (VPN) and firewalls, as necessary; and is compliant with IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)). (4.4)	N/A	N/A	N/A	N/A	
E. Estimate the percentage of the agency's network design and implementation that includes levels of redundancy, fault tolerance, and disaster recovery. (4.5)	N/A	N/A	N/A	N/A	
F. Estimate the percentage of the agency's network transport that complies with either Network Link Layer Access Protocol, or Ethernet, or IEEE 802.3, or the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method. (4.6)	N/A	N/A	N/A	N/A	
G. Estimate the percentage of the agency using Logical Network Topology, such as star or mesh, as appropriate. (4.7)	N/A	N/A	N/A	N/A	
H. Estimate the percentage of the agency using TCP/UCP and/or IP Transport and Network Layer Protocols. (4.8)	N/A	N/A	N/A	N/A	
I. Estimate the percentage of Network Devices (routers, switches, firewalls, access servers, etc.) that are securely deployed in accordance with applicable statewide IT security standards, and managed with network management platforms using the most current and approved open industry standard versions of Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON). (4.9)	N/A	N/A	N/A	N/A	
J. Estimate the percentage of Switching Technologies that are secure, in accordance with applicable statewide IT security standards, and used for LAN network device connectivity employing Open Systems Interconnection (OSI) Layers 2, 3, and 4. (4.10)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

K. Estimate the percentage of Routing Technologies used by the agency that are open and industry standards-based for Internet and inter-network connectivity, including the most current and approved versions of Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), etc. (4.11)	N/A	N/A	N/A	N/A	
L. Estimate the percentage of Converged Network Services, including LAN, WLAN, MAN, WMAN, And WAN, and/or accommodating secure (VPN & encryption) connectivity, transmission, and the convergence of voice, video, and data application traffic that the agency has implemented. (4.12)	N/A	N/A	N/A	N/A	
M. Estimate the percentage of Converged Services Client Platform Devices used by the agency capable of accepting and processing voice, video, and data applications within a single, secure, client platform device employing the most current and approved versions of open industry standards-based for signaling protocols. (4.13)	N/A	N/A	N/A	N/A	
N. Estimate the percentage of Inter-Network Transport Services, commonly referred to as Carrier Services, used by the agency that incorporate open, secure, scalable, industry standards-based packetized services; e.g., SONET, Frame Relay, ATM, etc., providing end-to-end quality of service capable of transporting voice, video, and data applications with a converged media stream. (4.14)	N/A	N/A	N/A	N/A	
O. Estimate the percentage of Internet-based Virtual Network Services that have been securely designed and implemented to include VPN technology as well as boundary and end-point security. (4.15)	N/A	N/A	N/A	N/A	
P. Estimate the percentage of VLAN Technologies implemented with converged network services segregating different types of network traffic, such as voice and data, and, as necessary, accessing applicable software applications. (4.16)	N/A	N/A	N/A	N/A	
Q. Estimate the percentage of Internal Network Interfaces using “private,” unregistered Internet Protocol (IP) addresses for network workstations and appliances using reserved addresses as defined by the Internet Assigned Numbers Authority (IANA). (4.17)	N/A	N/A	N/A	N/A	
R. Estimate the percentage of Internal Workstation Network IP Addresses assigned using Dynamic Host Configuration Protocol (DHCP). (4.18)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

S. Estimate the percentage of agency network systems using the Network Time Protocol (NTP) to securely obtain time information needed to synchronize network devices and computer clocks. (4.19)	N/A	N/A	N/A	N/A	

IT Planning for Platform Architecture	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Complian
S720 PLATFORM INFRASTRUCTURE					
A. Estimate the percentage of Server Platform target technologies (mainframe, midrange & network servers) implemented within the agency. (4.1, 4.2, 4.3, 4.4, 4.5)	N/A	N/A	N/A	N/A	
B. Estimate the percentage of Storage Platform target technologies(DAS, NAS, & SAN) implemented by the agency. (4.1, 4.2, 4.3, 4.4, 4.5)	N/A	N/A	N/A	N/A	
C. Estimate the percentage of Client Platform target technologies(PCs, thin client, PDAs, etc.) implemented by the agency. (4.1, 4.2, 4.3, 4.4, 4.5)	N/A	N/A	N/A	N/A	
D. Estimate the percentage of shared platform devices that are securely deployed in accordance with Statewide security standards, preventing unauthorized access and utilizing standard management tools compatible with SNMP. (4.6)	N/A	N/A	N/A	N/A	
E. Estimate the percentage of all portable platform devices capable of executing applications, storing information, and connecting to agency networks, that have been secured in accordance with P800-S820 Authentication and Directory Services and P800-S830 Network Security, as well as other applicable Statewide security standards. (4.10)	N/A	N/A	N/A	N/A	
F. Estimate the percentage of end-user devices used by third-parties, remote workers, and telecommuters that are secured in accordance with P800-S830 Network Security. (4.11)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

IT Planning for Software Architecture	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Compliance
S730 APPLICATIONS AND RELATED SOFTWARE					
A. Estimate the percentage of traditional, monolithic software applications (legacy mainframe software) greater than seven years old, still supporting agency programs that have been modified for improved interoperability, portability, and scalability. (4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	
B. Estimate the percentage of existing n-tier software applications supporting agency programs that have been modified for improved interoperability, portability, and scalability. (4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	
C. Estimate the percentage of traditional, monolithic or n-tier software applications supported and/or developed with browser or GUI-based client access to emphasize client productivity and performance. (4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	
D. Estimate the percentage of traditional, monolithic or n-tier software applications complying with Statewide IT Security Policy P800 and related security standards to safeguard the State's information and resources. (4.4)	N/A	N/A	N/A	N/A	
E. Estimate the extent to which the agency complies with the Statewide Intellectual Property Policy P252 and all legal provisions governing copyright laws and authorial integrity. (4.5)	N/A	N/A	N/A	N/A	
S731 SOFTWARE PRODUCTIVITY TOOLS					
F. Estimate the extent the agency complies with implementation of software productivity tools such as Email, Calendaring, etc., that allow for the exchange of data and information throughout the state as well as automation and support of agency business processes. (4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

IT Planning for Security	Currently (2006)	Planned by end of 2007	Planned by end of 2008	Planned by end of 2009	FY of 100% Compliance
S805 RISK MANAGEMENT					
A. Estimate the percentage of known IT risks and security vulnerabilities that are being tested by the agency each fiscal year. (4.1)	N/A	N/A	N/A	N/A	
S810 ACCOUNT MANAGEMENT					
B. Estimate the extent the agency complies with S810 standard for access and authorization of confidential information, levels of approval, special access privileges, system utilities, passwords, remote access, managing online and closed accounts of IT resources. (4.1, 4.2, 4.3, 4.4)	N/A	N/A	N/A	N/A	
C. Estimate the extent the agency complies with the S810 standard for Special Access Privileges, including high-level privileges (such as root access), system utilities, and privileges that provide access to sensitive network devices, operating systems, and software applications. (4.5)	N/A	N/A	N/A	N/A	
D. Estimate the extent the agency complies with S810 standard on the use of automated tools to coordinate and track Account Management activities for completeness and accuracy. (4.7)	N/A	N/A	N/A	N/A	
S815 CONFIGURATION MANAGEMENT					
E. Estimate the percentage of all IT devices and software assets maintained under configuration control. (4.1, 4.2)	N/A	N/A	N/A	N/A	
F. Estimate the percentage of network and system infrastructures possessing high-level and detailed network/systems diagrams that are baselined, maintained and current. (4.2.8)	N/A	N/A	N/A	N/A	
S820 AUTHENTICATION AND DIRECTORY SERVICES					
G. Estimate the percentage of critical network/systems, applications, and information safeguarded by the agency through Authentication by Knowledge before granting access to IT resources and services. (4.1, 4.3)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

H. Estimate the percentage of critical network/systems, applications, and information safeguarded by the agency through Authentication by Ownership before granting access to more sensitive IT resources and services. (4.1, 4.4)	N/A	N/A	N/A	N/A	
I. Estimate the percentage of critical network/systems, applications, and information safeguarded by the agency through Directory Services using Lightweight Directory Access Protocol (LDAP). (4.2)	N/A	N/A	N/A	N/A	
S825 SESSION CONTROLS					
J. Estimate the percentage of network client devices possessing automatic session/system timeouts based on inactivity, commensurate with the sensitivity of information. (4.1)	N/A	N/A	N/A	N/A	
K. Estimate the percentage of all client devices using locking screensavers with password-protection. (4.1)	N/A	N/A	N/A	N/A	
L. Estimate the extent to which the agency complies with S825 standard by locking online and remote accounts based on a maximum number of unsuccessful logon attempts. (4.3)	N/A	N/A	N/A	N/A	
M. Estimate the extent to which the agency complies with S825 standard by requiring system access logs to be turned on and maintained for a period of time determined by business needs. (4.4)	N/A	N/A	N/A	N/A	
S830 NETWORK SECURITY					
N. Estimate the percentage of the agency has implemented network perimeter security by employing firewall technologies and Internet gateways to protect sensitive information and infrastructure from unauthorized access, including wireless and portable devices. (4.1)	N/A	N/A	N/A	N/A	
O. Estimate the percentage of the agency using network traffic filtering rules and other security practices related to routing packets, destination addresses, security logs, encrypted traffic, and trusted peer relationship. (4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.9)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

P. Estimate the percentage of the agency using converged services (VoIP). (4.1.8)	N/A	N/A	N/A	N/A	
Q. Estimate the percentage of the agency that follows S830 standard by controlling and limiting access to internetworking devices (routers, firewalls, switches, etc.) and shared platforms (mainframes, servers, etc) to restrict both unauthorized access to and information about networks and infrastructure. (4.3)	N/A	N/A	N/A	N/A	
R. Estimate the percentage of the agency in compliance with S830 standard by using RFC 1928 and RFC 2827 for inbound Internet traffic and RADIUS for dial-in. (4.3, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.8)	N/A	N/A	N/A	N/A	
S. Estimate the percentage of the agency which complies with S830 standard by implementation of written patch management procedures for internetworking devices and shared platforms. (4.4) (P710-S710, 4.7)	N/A	N/A	N/A	N/A	
T. Estimate the percentage of the agency in compliance with S830 standard on routing external network connections through secure gateways and Transport Layer Security (TLS) or Secure Socket Layer (SSL). (4.6, 4.6.1)	N/A	N/A	N/A	N/A	
U. Estimate the percentage of agency compliance with S830 standard on routing wireless mobile devices through secure gateways and Wireless Transaction Layer Security (WTLS). (4.6, 4.6.2)	N/A	N/A	N/A	N/A	
V. Estimate the percentage of the agency compliance on routing external network connections through secure gateways and protected by Internet Protocol Security (IPSec). (4.6, 4.6.3)	N/A	N/A	N/A	N/A	
W. Estimate the percentage of the agency compliance with routing external network connections through secure gateways and protected by Virtual Private Network (VPNs). (4.6, 4.6.4)	N/A	N/A	N/A	N/A	

X. Estimate the percentage of agency compliance with routing dial-up modem connections through secure gateways and protected by Remote Authentication Dial-in User Service (RADIUS). (4.6, 4.6.5)	N/A	N/A	N/A	N/A	
Y. Estimate the percentage of agency compliance with written procedures for dial-up utilities and modems, disconnect and removal, tokens, authorization and authentication. (4.6, 4.6.6., 4.6.7, 4.6.8)	N/A	N/A	N/A	N/A	
Z. Estimate the percentage of the agency compliance with automatic re-routing of communications provided through transport services (Carrier Services), when critical nodes or links fail, using secure gateways. (4.7)	N/A	N/A	N/A	N/A	
AA. Estimate the percentage of the agency compliance with the use of IEEE standard 802.11x for wireless networks. (4.8, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5)	N/A	N/A	N/A	N/A	
AB. Estimate the percentage of agency compliance with the use of intrusion detection mechanisms and prevention tools on all internetworking devices that serve as gateways. (4.9)	N/A	N/A	N/A	N/A	
AC. Estimate the percentage of the agency in compliance with the use of network and system host vulnerability scanners to secure the agency infrastructure. (4.10)	N/A	N/A	N/A	N/A	
S850 ENCRYPTION TECHNOLOGIES					
AD. Estimate the percentage of agency compliance with the use of Public Key Infrastructure (PKI) for digital signatures having integrity, non-repudiation, and authentication. (4.1, 4.3, 4.4, 4.5, 4.8)	N/A	N/A	N/A	N/A	
AE. Estimate the percentage of agency compliance with the use of a symmetric cryptography (i.e., Open-PGP) for confidential electronic communications, data storage, and/or digital signatures. (4.2, 4.3, 4.4, 4.5.4.9)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

AF. Estimate the percentage of agency compliance with the use of Secure Multi-Purpose Internet Mail Extensions (S/MIME), in its most current version, to secure e-mail communications. (4.6)	N/A	N/A	N/A	N/A	
AG. Estimate the percentage of agency compliance with implementation of written procedures for PKI and Open-PGP to identify appropriate security levels of encryption, message integrity, and authentication. (4.7)	N/A	N/A	N/A	N/A	
AH. Estimate the percentage of the agency compliance with the Secretary of State's directive on PKI and PGP policy authority and electronic signature usage (A.R.S. 41-132). (4.10,4.11)	N/A	N/A	N/A	N/A	
S855 INCIDENT RESPONSE AND REPORTING					
AI. Estimate the percentage of the agency has complied with S855 standard by joining Statewide Infrastructure Protection Center (SIPC) for alert notifications and reporting incidents for the prevention of cyber-crime and terrorism at www.security.state.az.us/state-Infrastructure.htm. (4.1, 4.2, 4.3, 4.4, 4.5, 4.6)	N/A	N/A	N/A	N/A	
S860 VIRUS AND MALICIOUS CODE PROTECTION					
AJ. Estimate the percentage of the agency which has enabled 'notify and clean' by default for virus-scanning software of all servers, client workstations, and wireless devices. (4.1, 4.2)	N/A	N/A	N/A	N/A	
AK. Estimate the percentage of agency compliance with S860 standard by enabling virus-scanning software for storage devices including NAS and SAN. (4.3)	N/A	N/A	N/A	N/A	
AL. Estimate the percentage of agency which documents designated individuals as responsible and accountable for configuring and executing appropriate virus-scanning software, inoculants, and patches for network-attached and wireless workstations. (4.4)	N/A	N/A	N/A	N/A	
AM. Estimate the percentage of agency compliance with S860 standard by implementation of virus protection techniques for Instant Messaging (IM), Peer-to Peer (P2P) file-sharing and Internet Relay Chat (IRC) to guard against virus intrusions and malicious code. (4.9)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

S865 BUSINESS CONTINUITY AND DISASTER RECOVERY					
AN. Estimate the percentage of the agency which has developed a comprehensive Business Continuity and Disaster Recovery (BCDR) plan for the resumption of its critical public services based on unforeseen physical and/or system/cyber disasters. (5.0)	N/A	N/A	N/A	N/A	
AO. Estimate the percentage of critical business functions/applications that have been tested from an IT disaster recovery perspective within the last twelve months. (5.0)	N/A	N/A	N/A	N/A	
S870 BACKUPS					
AP. Estimate the percentage of the agency conducting automatic media backups on a periodic basis to support business processes, business continuity plans, legal mandates, regulatory, and contractual obligations. (4.0, 4.1, 4.2, 4.3)	N/A	N/A	N/A	N/A	
AQ. Estimate the percentage of the agency that stores removable backup media in a secure offsite location. (4.4)	N/A	N/A	N/A	N/A	
AR. Estimate the percentage of operating system software, application software, utilities, data/information, and security event logs included in backups for the configuration and restoration of critical agency information and services. (4.5)	N/A	N/A	N/A	N/A	
AS. Estimate the percentage of the agency possessing written procedures for conducting backups, transporting media, and testing backup media. (4.6)	N/A	N/A	N/A	N/A	
AT. Estimate the percentage of the agency that tests backups on a regular basis for restorability and recoverability. (4.7)	N/A	N/A	N/A	N/A	
S875 SYSTEM MAINTENANCE					
AU. Estimate the percentage of the agency possessing written change control procedures for hardware and software technologies upgrades, model types, version(s), and/or releases. (4.1)	N/A	N/A	N/A	N/A	

AV. Estimate the percentage of the agency having documented access control requirements and authorization of personnel having access to critical hardware, software, and network systems. (4.3)	N/A	N/A	N/A	N/A	
S880 MEDIA SANITIZING/DISPOSAL					
AW. Estimate the percentage of the agency that disposes of obsolete IT technologies through State Surplus; e.g., network components, platforms, storage devices, etc.. (4.0, 4.1)	N/A	N/A	N/A	N/A	
AX. Estimate the percentage of the agency compliance with final disposition of public/official records with public records statutes A.R.S. 38-421, 39-101, 39-121, 41-1345 through 1348, 41-1350 through 1351, and the Arizona Electronic Transaction Act A.R.S. 44-7041 of the Arizona State Library, Archives, and Public Records (ASLAPR) before obsolete technologies are sent to State Surplus. (4.0, 4.1)	N/A	N/A	N/A	N/A	
AY. Estimate the percentage of the agency that clears/deletes and verifies that data is unrecoverable from storage devices on platform and/or media devices before disposing through State Surplus. (4.2)	N/A	N/A	N/A	N/A	
AZ. Estimate the percentage of the agency that removes/clears/deletes all sensitive data prior to off-site repair of all IT devices with storage capabilities. (4.3)	N/A	N/A	N/A	N/A	
BA. Estimate the percentage of the agency that uses only authorized IT state/contract personnel for the clearing/deletion and removal of any sensitive data/information from IT technologies. (4.5)	N/A	N/A	N/A	N/A	
S885 PHYSICAL SECURITY					
BB. Estimate the percentage of the agency that secures all network components, mainframes, servers, and storage devices in primary locations, that are locked and restricted, and accessed only by authorized personnel (facility physical plant permitting). (4.1)	N/A	N/A	N/A	N/A	
BC. Estimate the percentage of the agency that uses appropriate fire suppression/prevention devices at primary facilities. (4.3)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

BD. Estimate the percentage of the agency possessing appropriate Uninterruptible Power Systems (UPS) for primary facilities. (4.3)	N/A	N/A	N/A	N/A	
BE. Estimate the percentage of the agency using appropriate backup generators for primary facilities. (4.3)	N/A	N/A	N/A	N/A	
S890 PERSONNEL SECURITY					
BF. Estimate the percentage of the agency that has implemented formal written security procedures identifying security administration accountability pertaining to unauthorized access and misuse of sensitive and confidential information. (4.1)	N/A	N/A	N/A	N/A	
BG. Estimate the percentage of the agency that has implemented formal written security procedures identifying the steps required to grant or withdraw physical and system access privileges for newly-hired State employees and/or contractors. (4.1)	N/A	N/A	N/A	N/A	
BH. Estimate the percentage of the agency that has implemented formal written security procedures identifying the steps required to grant or withdraw physical and system access privileges to State employees and contractors who have a change in job status/duties and/or transferred to another agency. (4.1)	N/A	N/A	N/A	N/A	
BI. Estimate the percentage of the agency that has implemented of formal written security procedures identifying the steps required to grant or withdraw physical and system access privileges to State employees and contractors who have submitted resignations, or terminated, or whose contracts have expired. (4.1)	N/A	N/A	N/A	N/A	
BJ. Estimate the percentage of the agency that has implemented formal written security procedures for requesting access to specific systems, applications, and/or data. (4.2)	N/A	N/A	N/A	N/A	
BK. Estimate the percentage of the agency that has provided non-disclosure agreements and applicable security agreements to state employees and contractors who require access to critical systems and confidential information. (4.4)	N/A	N/A	N/A	N/A	

TISA Assessment

2006

S895 SECURITY TRAINING AND AWARENESS					
BL. Estimate the percentage of the agency that provides IT security awareness training for its employees and contractors to address cyber and systems security, SIPC, technology, and data/information. (4.1, 4.2, 4.3, 4.4)	N/A	N/A	N/A	N/A	
S895 SECURITY SPECIFICS					
BM. Estimate the percentage of agency employees who have signed an 'appropriate use contract' which addresses Internet, email and network usage.	N/A	N/A	N/A	N/A	
BO. Estimate the percentage of the agency that has identified any third party Internet Service Providers (ISP) in use by the agency in its IT inventory.	N/A	N/A	N/A	N/A	